REMARKS

This communication is a full and timely response to the aforementioned final Office Action dated December 11, 2007. Reconsideration of the application and withdrawal of the rejections of the claims are respectfully requested in view of the following remarks.

I. Rejections under 35 U.S.C. § 103(a)

A. Claims 1, 4, 5, 7, 8, 10, 12, 17 and 20-25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Smetters in view of Benson (U.S. 6,047,242).

To establish a *prima facie* case of obviousness, the applied references must disclose or suggest all the claim limitations. See MPEP 2142; 706.02(j). If the applied references fail to disclose or suggest one or more of the features of a claimed invention, then the rejection is improper and must be withdrawn.

The rejection of claims 1, 4, 5, 7, 8, 10, 12, 17 and 20-25 is respectfully traversed for the following reasons.

(1) Independent Claims 1 and 7

Claim 1 recites a communication system in which a device and a client communicate data with each other through a network.

Claim 1 recites that the device comprises a first storage device which stores a root certificate including a public key paired with a private key, and that the root certificate is signed with the private key. Claim 1 recites that the device also comprises a certificate creator which creates a second certificate designating the root certificate as a certificate authority at a higher level.

Claim 1 also recites that the second certificate is signed with the private key. In addition, claim 1 recites that the device comprises a communication device which transmits the second certificate, which is created by the certificate creator and signed with the private key, to the client.

Claim 1 recites that the client comprises a second storage device which stores the root certificate stored in the first storage device. Further, claim 1 recites that the client comprises a verifier which verifies the signature of the second

certificate received from the device with the root certificate stored in the second storage device.

The invention of claim 1 provides an advantageous aspect of enabling the device and the client to securely communicate with each other through the network, without requiring either the device or the client to purchase an electronic certificate from an authority outside the network. This is achieved because the root certificate stored in the first storage device of the device is also stored in the second storage device of the client. The second certificate, which is signed by the private key, designates the root certificate as a certificate authority at a higher level. Accordingly, the verifier of the client can verify the signature of the second certificate with the root certificate that is stored in the second storage device of the client. Consequently, the client does not require a certificate issued by a third-party certificate authority or a certificate authority outside the network to verify the second certificate received from the device.

Claim 7 recites a method in which the device and client perform steps corresponding to the constituent elements of the communication system of claim 1.

The Office asserted that the features of claims 1 and 7 are disclosed in Smetters and Benson. The Office acknowledged that Smetters does not disclose or suggest the feature of creating a second certificate designating the root certificate as at a higher level, where the second certificate is signed with the private key included in the root certificate and used to sign the root certificate, as recited in claims 1 and 7. In an attempt to teach this feature, the Office applied Benson. However, Benson does not disclose or suggest this feature of claims 1 and 7 for the following reasons.

Benson discloses a software protection system in which a challenge means accesses a trusted root certificate. Benson discloses that a root certificate is used to authenticate a descendent certificate, which holds a public key of a trusted source. The descendent certificate is reached from the root certificate via a certificate path (see Column 2, lines 62-65 and Column 9, lines 46-55).

However, Benson discloses that "root certificates are signed using the certificate authority's private key" (see Column 2, lines 62-63) (emphasis added). Benson does not disclose or suggest that the descendent certificates are signed with

a private key of the certificate authority (CA), particularly a private key included in the root certificate and used to sign the root certificate, as recited in claims 1 and 7.

Claims 1 and 7 recite that the second certificate designates the root certificate as a certificate authority at a higher level. Accordingly, the second certificate recited in claims 1 and 7 corresponds to the "descendent certificate" of Benson.

However, Benson does not disclose or suggest that the descendent certificate is signed with a private key of the CA or a private key included in the root certificate. Instead, Benson discloses that the descendent certificate is reached (or validated) from the root certificate via a certification path, and that the descendent certificate holds a public key of a trusted source.

There is no support, either explicit or implicit, in Benson to support the Office's assertion that the descendant certificate is signed by a private key included in the root certificate and used to sign the root certificate, as recited in claims 1 and 7.

Therefore, in contrast to claims 1 and 7, neither Smetters nor Benson disclose or suggest the feature of creating a second certificate designating the root certificate as at a higher level, where the second certificate is signed with the private key included in the root certificate and used to sign the root certificate, as recited in claims 1 and 7. Such a feature is not disclosed, suggested or contemplated in Benson, contrary to the Office's assertion.

Furthermore, Applicant respectfully submits that modifying Smetters in the manner proposed by the Office to result in the subject matter of claims 1 and 7 would change a principle of operation of Smetters.

It is well-settled that if a modification of an applied reference would change the principle of operation of the reference being modified, then there is no reason, suggestion or motivation to modify the reference in that manner. See In re Ratti, 123 USPQ 349 (CCPA 1959); MPEP 2143.01.VI. Furthermore, it is well-settled that if a proposed modification of a reference would render the reference being modified unsatisfactory for its intended purpose, then there is no reason, suggestion or motivation to make the proposed modification. See In re Gordon, 221 USPQ 1125 (Fed. Cir. 1984); MPEP 2143.01.V.

In the present instance, Smetters discloses that a member certificate is signed with a public key, as will be described below. Despite this express disclosure, the Office proposed to substantially modify Smetters in an attempt to arrive at the subject matter of claims 1 and 7, but by doing so, the Office proposes to change a principle of operation of Smetters, which is improper and unsupportable.

Smetters discloses a system 10 for creating a shared resource space 20 containing resources 22, 24 to be shared among a first device 12(1) and a second device 12(2) (see Figures 1 and 3). The first device 12(1), which has access to the resources 22, 24, generates a root key pair to be used for authentication and encryption when providing the device 12(2) with access to the shared space 20 (see paragraph [0025], step 100 in Figure 2, and step 120 in Figure 4). In order to share access to the space 20, the first device 12(1) generates a root certificate 30 for the space 20 and digitally signs the root certificate 30 (see paragraph [0025], step 100 in Figure 2, and step 130 in Figure 4).

Then, the first device 12(1) sends an invitation message to the second device 12(2) and establishes a secure communication channel with the second device 12(2) by sending a range-limited signal including a public key used to secure the communication between the devices 12(1), 12(2) (see paragraphs [0028]-[0030], and steps 200 and 300 in Figure 2). Smetters discloses that the second device 12(2) then decides whether to use a particular public key (e.g., the public key included in the range-limited signal from the first device 12(1) or a public key generated by the second device 12(2) to communicate with the first device 12(1) (see paragraph [0032] and step 510 in Figure 6). If the second device 12(2) decides to use a particular public key, the second device 12(2) transmits this public key to the first device 12(1) (see paragraph [0032] and step 520 in Figure 6). On the other hand, if the second device 12(2) decides to use a public key generated by the first device 12(1), the first device 12(1) generates a pair of a public key and a private key, and sends the private key of the generated key pair to the second device 12(2) (see paragraph [0033], and steps 530 and 540 in Figure 6).

To provide the second device 12(2) with access to the shared space 20, Smetters discloses that the first device 12(1) then creates a second certificate 40 using either the public key sent from the second device 12(2) or the public key of the

key pair generated by the first device 12(1). The second certificate 40 designates the second device 12(2) as a member of the shared space 20 and is equivalent to the root certificate 30 (see paragraphs [0031] and [0034], step 500 in Figure 2, and step 550 in Figure 6).

Then, the first device 12(1) sends both the root certificate 30 and the second certificate 40 to the second device 12(2), and the second device 12(2) stores the received root certificate 30 and second certificate 40 in a memory thereof (see paragraph [0035] and step 600 in Figure 2). The root certificate 30 and the second certificate 40 stored in the second device 12(2) form a "certificate chain", which the second device 12(2) uses to prove to other devices 12(3) that the second device 12(2) is an authorized member of the shared space 20 (see paragraph [0035]). The "certificate chain" of the first device 12(1) is only the route certificate 30. If the second device 12(2) desires the first device 12(1) to verify that it is a legitimate provider of access to the space 20, the first device 12(1) presents its certificate chain (i.e., the root certificate 30) and proof of possession of the private key corresponding to the public key used to create the second certificate 40 to the second device 12(2) (see paragraph [0042]).

Smetters discloses that the second certificate 40 sent from the first device 12(1) to the second device 12(2) is signed with the public key that is transmitted from the second device 12(2) to the first device 12(1), or with the public key that is generated by the first device 12(1) (see paragraphs [0032], [0033] and [0041]). In the case where the second certificate 40 is created by using the public key generated by the first device 12(1), the first device 12(1) sends the corresponding private key to the second device 12(2), because the second device 12(2) requires the private key to access the second certificate 40.

Despite this express disclosure of Smetters, the Office has proposed to modify Smetters to arrive at the subject matter of claim 1. However, such a modification changes a principle of operation of Smetters and would also cause Smetters to be unsatisfactory for its intended purpose, i.e., allowing the second device 12(2) to access the second certificate 40.

Therefore, in addition to failing to disclose or suggest all the recited features of claims 1 and 7, the Office's proposed modification of Smetters would change a

principle of operation of Smetters and would render Smetters unsatisfactory for its intended purpose. As such, the proposed modification of Smetters is unwarranted and unsupportable, and therefore, one skilled in the art would not have been motivated to modify Smetters in the manner proposed by the Office.

Accordingly, for at least the foregoing reasons, Applicant respectfully submits that Smetters and Benson, either individually or in combination, fail to disclose or suggest all the recited features of claims 1 and 7. Furthermore, Applicant respectfully submits that there is no reason, suggestion or motivation to modify Smetters in the manner proposed by the Office, because the proposed modification would change a principle of operation of Smetters and would render Smetters unsatisfactory for its intended purpose.

Therefore, Applicant respectfully submits that claims 1 and 7 are patentable over Smetters and Benson.

(2) Dependent Claims of Claims 1 and 7

In addition to the patentability of independent claims 1 and 7, Applicant respectively submits that dependent claims 8 and 20-24 of claims 1 and 7 recite further distinguishing features over Smetters and Benson.

Claim 20 recites that the root certificate stored in the first storage device is stored in the second storage device prior to the transmission of the second certificate from the communication device. Claim 21 recites that the root certificate stored in the first storage device is stored in the second storage device prior to initiation of communication between the device and the client. Claim 23 recites that, in the method of claim 7, the device sends the second certificate to the client after the root certificate is installed in the client.

As described above, Smetters discloses that after the second device 12(2) has accepted the invitation from the first device 12(1), the first device 12(1) creates the second certificate 40 and then sends "both the root certificate 30 and the second laptop member certificate 40 to the [second device] 12(2)" (see paragraph [0035]) (emphasis added). Accordingly, since the first device 12(1) sends both the root certificate 30 and the second certificate 40 to the second device at the same time after the second certificate 40 is created, Smetters does not disclose or suggest the

above-described limitations of claims 20, 21 and 23. Benson also fails to disclose or suggest the limitations of claims 20, 21 and 23.

Claim 22 recites that the verifier of the client is operable to verify the signature of the second certificate by decrypting the public key of the root certificate stored in the second storage device to obtain a first hash value, calculating a second hash value of the second certificate received from the device, and comparing the first and second hash values to determine if they are equal to each other.

The Office asserted that the features recited in claim 22 are disclosed in paragraphs [0041] and [0042] of Smetters. This assertion is not supportable. Paragraphs [0041] and [0042] of Smetters do not disclose or suggest the calculation of the first and second hash values and the subsequent comparison of the first and second hash values, as recited in claim 22.

Claim 8 recites that the device further holds at least one intermediate certificate for one or more certificate authorities existing in a hierarchical order up to a root certificate authority. In addition, claim 8 recites that the client installs the at least one intermediate certificate in addition to the root certificate, and the device sends the second certificate to the client. Further, claim 8 recites that the client verifies the signature of the second certificate received from the device with the at least one intermediate certificate installed therein, and verifies the signature of the at least one intermediate certificate received from the device with the root certificate installed therein.

Claim 8 was rejected as being unpatentable over the combination of Smetters and Benson. In particular, the Office alleged that the limitations recited in claim 8 are disclosed by Smetters. Applicant respectfully submits that the Office has inconsistently interpreted the disclosure of Smetters in rejecting claim 8.

Smetters discloses that once the second device 12(2) has received both the root certificate 30 and the second certificate 40, the second device 12(2) may then give access to the shared space 20 to a third device 12(3). In effect, the second device 12(2) grants the third device 12(3) the access to the shared space 20 that it was granted by the first device 12(1) (see paragraph [0044]). After sending an invitation message and establishing a secure communication channel with the third device 12(3), the second device 12(3) creates a third certificate 50 for the third

device 12(3), and sends the "certificate chain" to the third device 12(3). Here, the "certificate chain" includes the root certificate 30 created by the first device 12(1), the second certificate 40 created by the first device 12(1) for the second device 12(2), and the third certificate 50 created by the second device 12(2) for the third device 12(3) (see paragraph [0045] and Figure 7).

By depending from claim 7, claim 8 further defines the limitations recited in claim 7. Claim 7 recites that the device creates and sends the second certificate to the client. Therefore, the "device" of claims 7 and 8 corresponds to the first device 12(1) of Smetters, and the "client" of claims 7 and 8 corresponds to the second device 12(2) of Smetters.

The second device 12(2) of Smetters cannot correspond to the "device" of claims 7 and 8, because the second device 12(2) does not create the second certificate 40, in contrast to claim 7. The second device 12(2) creates the third certificate 50, which is the lowest certificate in the hierarchy of the "certificate chain" received by the third device 12(3). On the other hand, the second certificate recited in claim 8 is the lowest certificate in the hierarchy of a certificate chain, because the client is recited in claim 8 as verifying the signature of the second certificate with the at least one intermediate certificate installed in the client, and verifying the signature of the at least one intermediate certificate with the root certificate installed in the client. Thus, the at least one intermediate certificate of claim 8 corresponds to the second certificate 40 of Smetters, and the second certificate of claim 8 corresponds to the third certificate 50 of Smetters.

However, in contrast to claim 8, the first device 12(1) of Smetters, which corresponds to the device of claim 8, does not send the third certificate 50 to the second device 12(2). Instead, as described above, the second device 12(2), independent of the first device 12(1), creates and sends the third certificate 50 (corresponding to the second certificate of claim 8) to the third device 12(3). Accordingly, Smetters does not disclose or suggest the step of the device sending the second certificate to the client, as recited in claim 8.

Furthermore, Smetters discloses that the third device 12(3) verifies the third certificate 50 by using the second certificate 40. Accordingly, Smetters also does not disclose or suggest that the client (second device 12(2)) verifies the signature of the

second certificate (third certificate 50) received from the device (first device 12(1)) with the at least one intermediate certificate (second certificate 40) installed therein, and verifies the signature of the at least one intermediate certificate (second certificate 40) received from the device (first device 12(1)) with the root certificate (root certificate 30) installed therein, as recited in claim 8.

Claim 24, which depends from claim 8, recites that the client installs the at least one intermediate certificate prior to receiving the second certificate from the device. Smetters does not disclose or suggest this limitation for two reasons. First, the second device 12(2) (client of claim 8) does not receive the third certificate 50 (corresponding to the second certificate of claim 8). Second, even if the second device 12(2) did receive the third certificate 50, the third certificate 50 is sent at the same time with the first and second certificates 30, 40 as a "certificate chain".

Accordingly, Applicant submits that Smetters does not disclose or suggest the features of claims 8 and 24. Benson also fails to disclose or suggest the features of claims 8 and 24.

For at least the foregoing reasons, Applicant submits that Smetters and Benson, either individually or in combination, do not disclose or suggest the features of claims 8 and 20-24.

Therefore, in addition to the patentability of claims 1 and 7 demonstrated above, Applicant respectfully submits that claims 8 and 20-24 are patentable over Smetters and Benson.

(3) Independent Claim 17

Claim 17 was identified in paragraph 8 on page 3 as being rejected over the combination of Smetters and Benson. However, the Office Action does not include a discussion of the features of claim 17, or the Office's application of Smetters and Benson with respect to the features of claim 17.

Nevertheless, Applicant respectfully submits that claim 17 is patentable over Smetters and Benson for the following reasons.

Claim 17 recites that the device comprises a certificate creator which creates a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key. As acknowledged by the Office,

Smetters fails to disclose or suggest this feature. The Office applied Benson in an attempt to teach this feature. However, as demonstrated above, Benson discloses that a root certificate, not a descendent certificate (second certificate), is signed with a private key. Accordingly, Smetters and Benson, either individually or in combination, do not disclose or suggest each and every limitation of claim 17.

Furthermore, Applicant respectfully submits that modifying Smetters to arrive at this feature would change a principle of operation of Smetters and would render Smetters unsatisfactory for its intended purpose, and therefore, is not supportable.

Therefore, Applicant respectfully submits that claim 17 is patentable over Smetters and Benson.

(4) Independent Claim 25

Claim 25 recites a device to be used in a communication system in which a device and a client communicate with each other through a network. Similar to claim 17, the device of claim 25 comprises a second storage device which stores a root certificate signed with the private key. The device of claim 25 also comprises a certificate creator which creates a second certificate designating the root certificate as a certificate authority at a higher level.

In addition, the device of claim 25 comprises an interface which sends the information as well as the root certificate including the public key to the client through the network, and sends, after the root certificate is installed in the client, the second certificate to the client for verification of the information sent from the device.

As described above, Smetters discloses that after the first device 12(1) creates the second certificate 40 for the second device 12(2), the first device 12(1) sends both the root certificate 30 and the second certificate 40 to the second device 12(2) as a "certificate chain" (see paragraph [0035]). Accordingly, in contrast to claim 25, Smetters does not disclose or suggest a device comprising an interface which sends, after the root certificate is installed in the client, the second certificate to the client for verification of the information sent from the device. Benson also fails to disclose or suggest this feature of claim 25.

Accordingly, for at least the foregoing reasons, Applicant submits that claim 25 is also patentable over Smetters and Benson, since Smetters and Benson, either

individually or in combination, do not disclose or suggest each and every feature of claim 25.

B. Dependent claims 2 and 3 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Smetters in view of Benson and further in view of Debry (U.S. 6,918,042). Dependent claims 9, 11, 18-19, 26 and 27 were rejected under 35 U.S.C. § 103(a) as unpatentable Smetters in view of Benson and Debry and further in view of Slick et al. (U.S. Patent Publication No. 2004/01109568, hereinafter "Slick"). Further, dependent claim 6 was rejected under 35 U.S.C. § 103(a) as unpatentable over Smetters and Benson and further in view of Vogel et al. (U.S. Patent No. 6,816,900, hereinafter "Vogel").

Without acquiescing to the Office's application of Debry, Slick and Vogel to the features of dependent claims 2, 3, 6, 9, 11, 18, 19, 26, 27, Applicant respectfully submits that Debry, Slick and Vogel, either individually or in combination, do not cure the deficiencies of Smetters and Benson for failing to disclose or suggest all the recited features of independent claims 1, 7, 17 and 25.

Therefore, no obvious combination of Smetters, Benson, Debry, Slick and Vogel would result in the subject matter of independent claims 1, 7, 17 and 25, as well as claims 2-6, 8-12, 1,8, 19, 20-24, 26 and 27 which depend therefrom, since these references, either individually or in combination, fail to disclose or suggest all the recited features of at least independent claims 1, 7, 17 and 25.

II. Rejections under 35 U.S.C. § 102(e)

Claims 13 and 16 were rejected under 35 U.S.C. § 102(e) as allegedly being anticipated over Smetters et al. (U.S. Patent Publication No. 2004/0088548, hereinafter "Smetters"). This rejection is respectfully traversed.

It is well-settled that a claim is anticipated only if each and every recited element is found, either expressly or inherently disclosed, in a single prior art reference. See Verdegal Bros. v. Union Oil Co. of California, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Thus, for a § 102 rejection to be proper, the cited reference must teach or suggest each and every recited feature in a claim, as well as the arrangement of the features recited in the claim. See MPEP 2131. Accordingly, if

the cited reference fails to disclose one or more of the recited features of a claim, then the rejection is improper and must be withdrawn.

Applicant respectfully submits that Smetters does not disclose or suggest all the recited features of claim 13 for the following reasons.

Claim 13 recites a computer-readable storage device storing a program which causes a computer to execute operations comprising requesting a root certificate from a device connected to the computer through a network, and receiving the root certificate from the device.

In addition, claim 13 recites that the program causes the computer to execute an operation of converting the received root certificate to a predetermined format upon receiving the root certificate, and an operation of installing the converted root certificate.

As described above, Smetters discloses a system 10 for creating a shared resource space 20 containing resources 22, 24 to be shared among a first device 12(1) and a second device 12(2), which may also share the resource space 20 with a third device 12(3) (see Figures 1 and 3).

In paragraph [0026], Smetters discloses that the system 10 according to the disclosed implementation utilizes standard cryptographic authentication techniques and creates a public key infrastructure ("PKI") to allow members of a shared space 20 to prove their membership to each other. However, Smetters notes that other authentication and cryptographic techniques may be used, such as group signature schemes, identity-based encryption, storage of lists of public keys or pre-existing certificates, shared secrets, or anonymous credentials. Furthermore, in paragraph [0026], Smetters discloses that in the disclosed implementation of the system 10, X.509 public key certificates are used. However, Smetters notes that the other certificate types, such as XML certificates, SPKI certificates, WTLS certificates or attribute certificates may be used.

Based on the disclosure of paragraph [0026], the Office asserted that "since different types of certificates can be used[,] it is well known in the art for any of these certificates to be converted to one standard in order to communicate with each other" (see lines 5-7 of paragraph 6 on page 3 of the Office Action) (emphasis added).

Accordingly, the Office is taking official notice of the supposed well-known converting operation recited in claim 13.

It is well-settled that official notice unsupported by documentary evidence should only be taken where the facts asserted to be well-known or common knowledge in the art are capable of instant and unquestionable demonstration as being well-known. The notice of facts beyond the record which may be taken by the Office must be "capable of such instant and unquestionable demonstration as to defy dispute." See In re Ahlert, 165 USPQ 418, 420 (CCPA 1970); MPEP 2144.03. Accordingly, it is improper to take official notice of facts without citing a prior art reference where the facts asserted to be well-known are not capable of instant and unquestionable demonstration as being well-known.

Despite these well-settled provisions, the Office asserted, without any supporting documentary evidence, that the converting operation of claim 13 is well-known in the art. The Office's allegation is based on the disclosure of paragraph [0026] of Smetters. However, paragraph [0026] of Smetters provides alternative cryptographic techniques that may be used instead of the techniques used in the described implementations.

Contrary to the Office's conclusory assertion, paragraph [0026] of Smetters does not disclose or suggest that it is well-known in the art to convert certificates formed in one technique to a certificate in another technique. In rejecting the claims of the present application, the Office applied a multifaceted combination of five different references. None of the five applied references provide support for the Office's unsupported and conclusory opinion that it is well-known in the art to convert one type of cryptographic certificate to another type of cryptographic certificate.

In the absence of documentary evidence to the contrary, Applicant submits that the ostensibly well-known feature of converting a certificate to a certificate of a different technique is not disclosed or suggested by any of the references of record.

Therefore, if the Office desires to maintain its interpretation that the converting operation and the subsequent installing operation as recited in claim 13 are "well known in the art," the Office is respectfully requested to produce actual documentary evidence of the ostensibly well-known features of claim 13.

In the Amendment filed on September 19, 2007, Applicant timely traversed the Office's assertion of official notice with respect to the converting operation recited in claim 13. However, the Office failed to produce any documentary evidence in the present Office Action.

Accordingly, contrary to the Office's unsupported assertion, Applicant respectfully submits that Smetters and the other applied references do not disclose, suggest or contemplate the converting operation recited in claim 13. Furthermore, Applicant respectfully submits that Smetters and the other applied references do not support, in any reasonable way, the Office's assertion that the converting operation of claim 13 is well-known in the art.

Therefore, for at least the foregoing reasons, Applicant respectfully submits that the converting operation and the subsequent operation of installing the converted certificate, as recited in claim 13, are not disclosed or suggested by Smetters, or any of the other applied references.

Consequently, Applicant respectfully submits that claim 13, as well as claims 15 and 16 which depend therefrom, are patentable over Smetters and the other references of record.

For at least the foregoing reasons, Applicant respectfully submits that Smetters, Benson, Debry, Slick and Vogel, either individually or in combination, do not disclose or suggest all the recited features of independent claims 1, 7, 13, 17 and 25.

Therefore, no obvious combination of Smetters, Benson, Debry, Slick and Vogel would result in the subject matter of claims 1, 7, 13, 17 and 25, since these references, either individually or in combination, fail to disclose or suggest all the recited features of claims 1, 7, 13, 17 and 25.

Furthermore, in view of the distinctions discussed above, one skilled in the art would not have reason or been motivated to modify the applied references in such a manner as to result in, or otherwise render obvious, the subject matter of claims 1, 7, 13, 17 and 25.

Accordingly, Applicant respectfully submits that claims 1, 7, 13, 17 and 25, as well as claims 2-6, 8-12, 15, 16, 18-24, 26 and 27 which depend therefrom, are patentable over the applied references.

The foregoing explanation of the patentability of independent claims 1, 7, 13, 17 and 25 is sufficiently clear such that it is believed that separately arguing the patentability of the dependent claims whose rejections were not traversed above is unnecessary at this time. However, Applicant reserves the right to do so if it becomes appropriate.

III. Conclusion

In view of the foregoing remarks, it is respectfully submitted that the present application is clearly in condition for allowance. Accordingly, Applicant requests a favorable examination and consideration of the instant application.

If, after reviewing this Response, the Examiner feels there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: May 2, 2008

By: /Jonathan Bowser/
Jonathan R. Bowser
Registration No. 54574

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620